On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities

Colas Le Guernic, Mohab Safey El Din

▶ **To cite this version:**

Colas Le Guernic, Mohab Safey El Din. On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities. [Research Report] RR-5079, INRIA. 2004. inria-00071504

HAL Id: inria-00071504
https://inria.hal.science/inria-00071504

Submitted on 23 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities

Colas Le Guernic — Mohab Safey El Din

N° 5079

Janvier 2004

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--5079--FR+ENG

INRIA
ROCQUENCOURT

On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities

Colas Le Guernic , Mohab Safey El Din

Thème 2 — Génie logiciel
et calcul symbolique
Projet SPACES

Rapport de recherche n° 5079 — Janvier 2004 — 15 pages

Abstract: Given polynomials $f_1, \ldots, f_k, g_1, \ldots, g_s$ in $\mathbb{Q}[X_1, \ldots, X_n]$, we consider the semi-algebraic set $\mathcal{S}$ defined by:

$$f_1 = \ldots = f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

and focus on the problem of computing at least one point in each connected component of $\mathcal{S}$. We first study how to solve this problem by considering $\mathcal{S}$ as the union of solutions sets of polynomial systems of equations and strict inequalities and proceed to the complexity analysis of the underlying algorithm. Then, we improve this approach by proving that computing at least one point in each connected component of $\mathcal{S}$ can be done by computing at least one point in each connected component of real algebraic sets defined by vanishing the polynomials $f_1, \ldots, f_k$ and some of the polynomials $g_1, \ldots, g_s$. The complexity analysis shows that this latter approach is better than the former one. Finally, we present our implementation and use it to solve an application in Pattern Matching.

Key-words: Polynomial systems, Real solutions, non-strict inequalities

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex (France)
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

Sur le calcul d'au moins un point par composante connexe d'un semi-algébrique défini par un système polynomial d'équations et d'inégalités larges

Résumé : Soient $f_1, \ldots, f_k, g_1, \ldots, g_k$ dans $\mathbb{Q}[X_1, \ldots, X_n]$, considérons l'ensemble semi-algébrique $\mathcal{S}$ défini par:

$$f_1 = \ldots, f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

Notre problème est de calculer au moins un point par composante connexe de $\mathcal{S}$. Ce problème peut être résolu en considérant l'union de l'ensemble des solutions de plusieurs systèmes d'équations et d'inégalité strictes. Nous montrons qu'en fait, il suffit de considérer les ensembles de solutions de plusieurs systèmes d'équations polynomiales. Cette méthode a une meilleure complexité que la précédente. Finalement nous présenterons une implémentation de l'algorithme et une application au pattern matching.

Mots-clés : Systèmes polynomiaux, Solutions réelles, Inégalités larges

1 Introduction

Polynomial systems of equations and inequalities appear in many fields like computer aided design, signal theory, robotics, and pattern matching. Deciding the emptiness, and computing at least one point in each connected component of the solution set of such systems is consequently a fundamental algorithmic problem in effective real algebraic geometry. This paper proposes an *efficient* algorithm computing at least one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and *non-strict* inequalities. We present its implementation and apply it to a problem coming from pattern matching which is, up to our knowledge, intractable by the other existing implementations dealing with semi-algebraic sets.

Related works The problem of computing at least one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and *non-strict* inequalities is not specifically addressed in the literature, since it can be naively reduced to the problem of computing at least one point in each connected component of several semi-algebraic sets defined by polynomial systems of equations and *strict* inequalities.

A widespread algorithm taking as input a polynomial system of equations and inequalities and computing at least one point in each connected component of the solution set of the input system is the well-known cylindrical algebraic decomposition algorithm due to Collins and his collaborators (see [12]). Its complexity is doubly exponential in the number of variables of the studied polynomial family, and the best implementations of this algorithm are limited to non-trivial problems having less than 5 variables.

Since the two last decades, several algorithms with a single exponential theoretical complexity in the number of variables have been proposed (see [18, 19, 20, 7, 8, 9, 24]). These works culminate with the results of Basu, Pollack and Roy, provided in a unified way in [10], where the complexity of computing at least one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and strict inequalities is decomposed into a combinatorial factor and an algebraic one. Most of the aforementioned algorithms rely on a geometrical result allowing to reduce the case of a polynomial system of equations and strict inequalities to the computation of at least one point in each connected component of several real algebraic varieties defined by polynomial systems with coefficients in a *Puiseux series field*. We recall now, how to deal with this step.

Computation of one point in each connected component of a real algebraic set Optimal algorithms computing at least one point in each connected component of a real algebraic set are based on the critical point method. This consists in computing the critical locus, supposed to be *zero-dimensional*, of a mapping, which is supposed to reach its extrema on each connected component of the studied real algebraic set.

This method is used in [18, 19, 20, 7, 8, 9, 24] to obtain algorithms which are polynomial in a Bézout-like bound. Nevertheless, to deal with non-compact and non-smooth cases some infinitesimals and algebraic manipulations are introduced and they do not allow to obtain efficient implementations: they make heavier the arithmetic on which the computations are performed and lead to consider *systematically* zero-dimensional polynomial systems whom degrees are Bézout-like. This prevents to give *intrinsic* geometric degree bounds.

The problem is tackled with a view toward practical efficiency in [2, 29] by using the distance function, and in [32] by using projection functions, and no complexity estimates is given.

In [4, 3], the authors use the elimination procedures provided in [16, 14, 15, 17, 21] to obtain an algorithm which is polynomial in an *intrinsic* geometric degree bound and which computes at least one point in each connected component of a *smooth and compact* real algebraic set defined by a regular sequence.

These complexity results are generalized to non-compact situations in [31] using projection function and in [6, 5], where the authors go back to the distance function. We use in the sequel the complexity result given in [31] that we recall now. We denote by $\mathcal{M}(x)$ the number of operations required to multiply polynomials of degree x and the notation $f \in \mathcal{O}_{\log}(x)$ means that $f \in \mathcal{O}(x \log(x)^a)$ for some constant a.

Theorem 1 *[31] Let $(f_1, \ldots, f_k)$ be a polynomial family in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree bounded by D generating a radical and equidimensional ideal of dimension d and defining a smooth algebraic variety $\mathcal{V}$. Let S denote the combinatorial number $S = \binom{k}{n-d}.\binom{n-1}{n-d}$ and G denote the polynomial family*

$$f_1, \ldots, f_k, M_{1,1}, \ldots, M_{1,S}$$

where $(M_{i,j})$ is a sequence of the $(n-d, n-d)$ minors of the jacobian matrix associated to $(f_1, \ldots, f_k)$ with respect to the variables $X_1, \ldots, X_n$.

Let δ be an integer bounding the algebraic degree of any prefix subsequence of the polynomial family G. There exists a probabilistic algorithm computing at least one point in each connected component of $\mathcal{V} \cap \mathbb{R}^n$ whose complexity is within

$$\mathcal{O}_{\log}(Ln^{10}S(k+S)\mathcal{M}(D(n-d)\delta)^3)$$

arithmetic operations.

All these algorithms return zero-dimensional systems whose real solutions can be found by computing a rational parametrization of their complex solution set using the algorithms provided in either [1, 25] or [16, 14, 15, 17, 21]. We refer to [27] for the isolation of real roots of a univariate polynomial with coefficients in an archimedean field using Uspensky's algorithm and [10] (and references therein) for the same task on Puiseux series fields using Sturm-Habicht sequences.

Contributions We focus on polynomial systems of equations and *non-strict* inequalities.

All along the paper, we consider polynomials $f_1, \ldots, f_k$ and $g_1, \ldots, g_s$ in $\mathbb{Q}[X_1, \ldots, X_n]$ for some k, s and n in $\mathbb{N}$ and the semi-algebraic set $\mathcal{S} \subset \mathbb{R}^n$ defined by:

$$\begin{array}{l} f_1 = \ldots = f_k = 0 \\ g_1 \geq 0, \ldots, g_s \geq 0 \end{array}$$

As mentioned above, the solution set of such a polynomial system of equations and *non-strict* inequalities is the union of the solution sets of polynomial systems of equations and *strict* inequalities:

$$\left\{ \begin{array}{l} f_1 = \ldots = f_k = 0 \\ g_{i_1} = \ldots = g_{i_\ell} = 0 \\ g_j > 0 \quad \forall j \notin \{i_1, \ldots, i_\ell\} \end{array} \right.$$

for all subset $\{i_1, \ldots, i_\ell\}$ of $\{1, \ldots, s\}$.

Thus, computing at least one point in each connected component of $\mathcal{S}$ can be done by computing at least one point in each connected component of the semi-algebraic sets defined by the above polynomial systems. Using the results of [8, 9, 10] and [31], this leads to an algorithm whose complexity is a sum of products decomposed into a combinatorial factor and the power of an *intrinsic* geometric degree bound. The arithmetic operations are here counted in a Puiseux series field since the use of results of [8, 9, 10] induces the introduction of an infinitesimal.

Our main result consists in reducing the computation of at least one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and *non-strict* inequalities to the computation of at least one point in each connected component of several *real algebraic sets* defined by polynomials with coefficients in $\mathbb{Q}$. More precisely, we prove that computing at least one point in each connected components of $\mathcal{S}$ can be done by computing at least one point in each connected component of the real algebraic sets defined by:

$$f_1 = \ldots = f_k = 0$$
$$g_{i_1} = \ldots = g_{i_\ell} = 0$$

for all subset $\{i_1, \ldots, i_\ell\}$ in $\{1, \ldots, s\}$. Thus, the infinitesimal deformation introduced in the preceding approach is avoided and the number of arithmetic operations performed by the underlying algorithm is counted over $\mathbb{Q}$. Compared to the preceding approach, we show this allows to reduce the combinatorial factors, while the algebraic ones are still polynomial in some *intrinsic* geometric degree bounds.

We then present an implementation of this algorithm, which will be integrated in the next release of the RAGLib Maple Library [30] and show how it can be applied to a problem coming from pattern matching.

Organization of the paper In the following section, we show how to tackle polynomial systems of equations and *non-strict* inequalities by considering polynomial systems of equations and *strict* inequalities. We proceed a complexity analysis of the algorithm induced by this naive approach, in some generic cases. In next section, we show how to tackle the same problem by solving exclusively polynomial systems of equations. We show how this improve the complexity of the new obtained algorithm which is successfully applied in the last section to a pattern matching problem.

2 A first approach

In this section, we show how finding at least one point in each connected component of a semi-algebraic set defined by equations and *non-strict* inequalities is reduced to finding at least one point in each connected component to several semi-algebraic sets defined by equations and *strict* equalities.

Proposition 1 *Let $(f_1, \ldots, f_k, g_1, \ldots, g_s)$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$, $\mathcal{S} \subset \mathbb{R}^n$ be the semi-algebraic set defined by:*

$$f_1 = \ldots = f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

and S be a connected component of $\mathcal{S}$.

Then, there exists a subset $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$ *such that the semi-algebraic set defined by:*

$$\begin{cases} f_1 = \ldots = f_k = 0 \\ g_{i_1} = \ldots = g_{i_\ell} = 0, \\ g_j > 0 \quad \forall j \in \{1, \ldots, s\} \setminus \{i_1, \ldots, i_\ell\} \end{cases}$$

has a connected component S' *included in* S.

Proof. Let y be a point of $S \subset \mathcal{S}$ and $\{i_1, \ldots, i_\ell\}$ the set of indices of polynomials of $\{g_1, \ldots, g_s\}$ that vanish in y. Let S' be the semi-algebraic connected component of the semi-algebraic set by:

$$\begin{cases} f_1 = \ldots = f_k = 0 \\ g_{i_1} = \ldots = g_{i_\ell} = 0, \\ g_j > 0 \quad \forall j \in \{1, \ldots, s\} \setminus \{i_1, \ldots, i_\ell\} \end{cases}$$

such that $y \in S'$. For any point $y' \in S'$, there exists a continuous semi-algebraic path $\gamma : [0,1] \to S'$ such that $\gamma(0) = y$ and $\gamma(1) = y'$. Since for all $t \in [0,1]$, $\gamma(t) \in S'$, for all $t \in [0,1]$ and all $j \in \{1, \ldots, s\} \setminus \{i_1, \ldots, i_\ell\}$, $g_j(t)$ does not vanish on $\gamma(t)$ and is consequently positive on this path since $g_j(\gamma(0)) > 0$. Thus, $S' \subset S$.

□

Thus the problem of computing at least one point in each connected component of a semi-algebraic set defined by equations and non-strict inequalities is reduced to computing at least one point in each connected component of several semi-algebraic sets defined by equations and strict inequalities. As mentioned in the introduction, this problem is tackled by asymptotically optimal algorithms, in particular those of Basu, Pollack and Roy based on the following geometric result:

Theorem 2 *[8, 9, 10] Let* $(f_1, \ldots, f_k, g_1, \ldots, g_s)$ *be a polynomial family in* $\mathbb{Q}[X_1, \ldots, X_n]$ *and* S *be a connected component of the semi-algebraic set defined by:*

$$f_1 = \ldots = f_k = 0, \quad g_1 > 0, \ldots, g_s > 0$$

Then, there exist $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$ *such that the real counterpart of the algebraic variety defined by:*

$$f_1 = \ldots = f_k = g_{i_1} - \varepsilon = \ldots = g_{i_\ell} - \varepsilon = 0$$

has a connected component included in S.

This result reduces the problem of finding at least one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and strict inequalities with coefficients in $\mathbb{Q}$ to the problem of finding at least one point in each connected component of a real algebraic set defined by a polynomial system of equations with coefficients in $\mathbb{Q}\langle\varepsilon\rangle$, using for example the algorithms provided in [2, 29, 31]. In the sequel, we denote by `Components` a routine taking as input a polynomial system of equations in $\mathbb{Q}[X_1, \ldots, X_n]$ and returning an encoding of at least one point in each connected component of the real algebraic set defined by the input system, under the form of a list of rational parameterizations with coefficients in $\mathbb{Q}(\varepsilon)$ of the complex solution sets of zero-dimensional systems.

Following [8, 9, 10], the sign of a polynomial $g \in \mathbb{Q}[X_1, \ldots, X_n]$ at each real point of a zero-dimensional system can be computed from such an encoding, by pseudo-remainder computations to reduce the multivariate problem to a univariate one and by isolating the real roots

of univariate polynomials with coefficients in $\mathbb{Q}(\varepsilon)$. Below, we denote by `TestSign` a subroutine taking as input a list of parameterizations with coefficients in $\mathbb{Q}(\varepsilon)$ and a list of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ which returns the parameterizations encoding real points on which *all* the polynomials of the second input list are positive.

Algorithm 1

- **Input** : two lists of polynomials $\{f_1, \ldots, f_k\}$, and $\{g_1, \ldots, g_s\}$ in $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Output** : an encoding of at least one point in each connected components of the semi-algebraic set defined by:
$$f_1 = \ldots = f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

1. $result \leftarrow \emptyset$
2. **For all** $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$
   - For all $\{j_1, \ldots, j_p\} \subset \{1, \ldots, s\} \setminus \{i_1, \ldots, i_\ell\}$
   - $UR \leftarrow$ `Components`$([f_1, \ldots, f_k, g_{i_1}, \ldots, g_{i_\ell}, g_{j_1} - \varepsilon, \ldots, g_{j_p} - \varepsilon])$
   - $result \leftarrow$ `TestSign`$(UR, \{g_j \mid j \in \{1, \ldots, s\} \setminus \{i_1, \ldots, i_\ell, j_1, \ldots, j_p\}) \cup result$
3. return $result$

Complexity analysis Our complexity analysis is based on [31, Theorem 3]. The arithmetic complexity of **Algorithm** 1 is the arithmetic complexity of `Components` multiplied by the number of possible choices for $\mathcal{I}$ and $\mathcal{J}$, i.e. $\sum_{i=0}^{s} \binom{s}{i}.2^{s-i}$.

Theorem 3 *Let $(f_1, \ldots, f_k, g_1, \ldots, g_s)$ be polynomials of degree bounded by D in $\mathbb{Q}[X_1, \ldots, X_n]$, and $\mathcal{S} \subset \mathbb{R}^n$ be the semi-algebraic set defined by:*

$$f_1 = \ldots = f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

Given any subset $\mathcal{I} = \{i_1, \ldots, i_\ell\}$ of $\{1, \ldots, s\}$, and $\mathcal{J}$ a subset of $\{1, \ldots, s\} \setminus \mathcal{I}$, let $F_{\mathcal{I},\mathcal{J}}$ denote the polynomial family

$$(f_1, \ldots, f_k, g_{i_1}, \ldots, g_{i_\ell}, g_{j_1} - \varepsilon, \ldots, g_{j_p} - \varepsilon),$$

$d_{\mathcal{I},\mathcal{J}}$ denote the dimension of the algebraic variety defined by $F_{\mathcal{I},\mathcal{J}}$, $C_{\mathcal{I},\mathcal{J}}$ the combinatorial number $\binom{k+|\mathcal{I}|+|\mathcal{J}|}{n-d_{\mathcal{I},\mathcal{J}}}.\binom{n}{n-d_{\mathcal{I},\mathcal{J}}}$, $L_{\mathcal{I},\mathcal{J}}$ denote the length of a Straight Line program evaluating $F_{\mathcal{I},\mathcal{J}}$, and $\delta_{\mathcal{I},\mathcal{J}}$ the algebraic degree associated to $F_{\mathcal{I},\mathcal{J}}$ in Theorem 1.

Assume that for any subsets $\mathcal{I}$ and $\mathcal{J}$, $F_{\mathcal{I},\mathcal{J}}$ generates a radical and equidimensional ideal and defines a smooth algebraic variety. There exists a probabilistic algorithm computing at least one point in each connected component of $\mathcal{S}$ with an arithmetic complexity within

$$\sum_{\substack{\mathcal{I} \subset \{1, \ldots, s\} \\ \mathcal{J} \subset \{1, \ldots, s\} \setminus \mathcal{I}}} \mathcal{O}_{\log}(L_{\mathcal{I},\mathcal{J}} n^{10} C_{\mathcal{I},\mathcal{J}} (k + |\mathcal{I}| + |\mathcal{J}| + C_{\mathcal{I},\mathcal{J}}) \mathcal{M}((n - d_{\mathcal{I},\mathcal{J}}) D \delta_{\mathcal{I},\mathcal{J}})^3)$$

arithmetic operations in $\mathbb{Q}\langle\varepsilon\rangle$.

In the following section, we show how to reduce this complexity, by providing an algorithm studying exclusively polynomial systems with coefficients in $\mathbb{Q}$ and studying less polynomial systems than **Algorithm** 1.

3 Our algorithm

In this section, we show how to reduce the problem of finding at least one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non strict inequalities with coefficients in $\mathbb{Q}$ to the problem of finding at least one point in each connected component of several real algebraic sets defined by polynomial systems of equations with coefficients in $\mathbb{Q}$.

The result allowing such a reduction is based on the following intuition: if a polynomial Q is positive and negative on a connected component of an algebraic set V, then by the intermediate value theorem, it vanishes on this component and then one can study $V \cap V(Q)$.

The result below is similar to [28, Proposition 6.17] (see also [8, 9, 10]) and its proof is based on the same principles.

Theorem 4 *Let $(f_1, \ldots, f_k, g_1, \ldots, g_s)$ be a polynomial family in $\mathbb{Q}[X_1, \ldots, X_n]$, $\mathcal{S} \subset \mathbb{R}^n$ be the semi-algebraic set defined by:*

$$\begin{cases} f_1 = \ldots = f_k = 0 \\ g_1 \geq 0, \ldots, g_s \geq 0 \end{cases}$$

and S be a connected component of $\mathcal{S}$.
Then there exists $\{i_1, \ldots, i_\ell\}$ such that the algebraic variety defined by:

$$f_1 = \ldots = f_k = g_{i_1} = \ldots = g_{i_\ell} = 0$$

has a connected component C included in S.

Proof. Consider $\{i_1, \ldots, i_\ell\}$ be a maximal subset for inclusion of

$$\{I \subset \{1, \ldots, s\} \mid \exists x \in S, \forall i \in I, g_i(x) = 0\}$$

and denote by V the real algebraic variety defined by:

$$f_1 = \ldots = f_k = g_{i_1} = \ldots = g_{i_\ell} = 0$$

Let C_0 denote a connected component of $S \cap V$ and C the connected component of V containing C_0. Remark that, since $\{i_1, \ldots, i_\ell\}$ is maximal, any polynomial g_i for $i \notin \{i_1, \ldots, i_\ell\}$ do *never* vanish on C_0. We show now that $C = C_0$, which will establish a proof of the theorem.

First remark that by definition of C, $C_0 \subset C$. Consider now x_0 a point in C_0 and x_1 a point in C. Let γ be a semi-algebraic path from x_0 to x_1 in C and consider $\mathcal{Z}$ as the set of polynomials that vanish in $\gamma([0,1])$.

Suppose $\mathcal{Z}$ to be non-empty. For any polynomial g in $\mathcal{Z}$, $g \circ \gamma$ is algebraic and vanishes on a finite number of point in $[0,1]$ (or is identically zero on $[0,1]$). Moreover, by definition of $\mathcal{Z}$, $g \circ \gamma$ vanishes on at least one point in $[0,1]$. Thus, one can define θ_g^γ the least vanishing point of $g \circ \gamma$ in $[0,1]$. Then, as $\mathcal{Z}$ is finite, one can define θ the least θ_g^γ for g in $\mathcal{Z}$.

Any polynomial in $\{g_1, \ldots, g_s\}$ is zero or positive on the path $\gamma([0,\theta])$, and there exists a polynomial g^θ in $\mathcal{Z}$ (if it is not empty) that vanishes on $\gamma(\theta)$.

Thus $\gamma(\theta)$ is a point of S on which $g^\theta, g_{i_1}, \ldots$, and g_{i_ℓ} vanish, which is not possible from the definition of $\{i_1, \ldots, i_\ell\}$. Therefore no polynomial in $\{g_{i_{\ell+1}}, \ldots, g_{i_s}\}$ vanishes on γ and x_1 belongs to C_0, which implies that $C \subset C_0$ and ends the proof.

□

Thus, to compute at least one point in each connected component of a semi-algebraic set $\mathcal{S}$ defined by a polynomial system of equations and *non-strict* inequalities with coefficients in $\mathbb{Q}$, it is enough to compute one point in each connected component of the real counterparts of some algebraic sets defined by polynomial systems with coefficients in $\mathbb{Q}$.
As in the preceding paragraph, we use subroutines called `Components` and `TestSign` to compute at least one point in each connected component of a real algebraic set and select among a list of rational parameterizations those encoding at least one real point on which some given polynomials are positive.

Algorithm 2

- **Input** : two lists of polynomials $\{f_1, \ldots, f_k\}$, and $\{g_1, \ldots, g_s\}$ in $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Output** : an encoding of at least one point in each connected components of the semi-algebraic set defined by:
$$f_1 = \ldots = f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

1. $result \leftarrow \emptyset$
2. **For all** $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$
   - $UR \leftarrow$ `Components`$([f_1, \ldots, f_k, g_{i_1}, \ldots, g_{i_\ell}])$
   - $result \leftarrow$ `TestSign`$(UR, \{g_j \mid j \in \{1, \ldots, s\} \setminus \{i_1, \ldots, i_\ell\}\}) \cup result$
3. return $result$

Complexity Analysis Our complexity analysis is still based on Theorem 1 (see [31]).

Algorithm 2 calls the subroutine `Components` for each subset of $\{1, \ldots, s\}$, i.e. 2^s times. In the case where each polynomial family studied by our algorithm verifies the assumptions of Theorem 1, one can estimate the complexity of **Algorithm** 2 (where the number of operations is counted in $\mathbb{Q}$).

Theorem 5 *Let $(f_1, \ldots, f_k, g_1, \ldots, g_s)$ be polynomials of degree bounded by D in $\mathbb{Q}[X_1, \ldots, X_n]$, and $\mathcal{S} \subset \mathbb{R}^n$ be the semi-algebraic set defined by:*

$$f_1 = \ldots = f_k = 0$$
$$g_1 \geq 0, \ldots, g_s \geq 0$$

Given any subset $\mathcal{I} = \{i_1, \ldots, i_\ell\}$ of $\{1, \ldots, s\}$, let $F_\mathcal{I}$ denote the polynomial family $(f_1, \ldots, f_k, g_{i_1}, \ldots, g_{i_\ell})$, $d_\mathcal{I}$ denote the dimension of the algebraic variety defined by $F_\mathcal{I}$, $C_\mathcal{I}$ the combinatorial number $\binom{k+|\mathcal{I}|}{n-d_\mathcal{I}}.\binom{n}{n-d_\mathcal{I}}$, $L_\mathcal{I}$ denote the length of a Straight Line program evaluating $F_\mathcal{I}$, and $\delta_\mathcal{I}$ the algebraic degree associated to $F_\mathcal{I}$ in Theorem 1.

Assume that for any subset $\mathcal{I}$, $F_{\mathcal{I}}$ generates a radical and equidimensional ideal and defines a smooth algebraic variety. There exists a probabilistic algorithm computing at least one point in each connected component of $\mathcal{S}$ with an arithmetic complexity within

$$\sum_{\mathcal{I}\subset\{1,\ldots,s\}} \mathcal{O}_{\log}(L_{\mathcal{I}} n^{10} C_{\mathcal{I}}(k+|\mathcal{I}|+C_{\mathcal{I}})\mathcal{M}((n-d_{\mathcal{I}})D\delta_{\mathcal{I}})^3)$$

arithmetic operations in $\mathbb{Q}$.

This complexity is clearly better than the one obtained for **Algorithm** 1: this algorithm studies more polynomial systems than **Algorithm** 2. Moreover, remark that if we assume additionally that for each $\mathcal{I} \subset \{1,\ldots,s\}$, the polynomial family $F_{\mathcal{I}}$ defines a regular sequence, then one has only to consider the subsets $\mathcal{I}$ containing at most d indices where d denotes the dimension of the algebraic variety defined by:

$$f_1 = \ldots = f_s = 0.$$

4 Application to pattern matching and experimental results

Description of the problem Let $\mathcal{P}$ and $\mathcal{Q}$ be two geometric objects in an euclidean space E, with a distance function d over such objects, and G a group of transformations. Given a real positive number ϵ, the typical geometric pattern matching problem is to decide if there exists a transformation g in G such that $d(\mathcal{P}, g\mathcal{Q}) < \epsilon$.

To describe our specific problem we need the following notations and definitions. First, a polygonal curve $\mathcal{P}$ is a function from $[0:m]$ to $\mathbb{R}^3$ such as $\mathcal{P}(i) = p_i$ is the i^{th} vertex of $\mathcal{P}$.

Notation 1 *We denote by $Mon(X,Y)$ the set of all non-strictly increasing surjective mappings from a set X to a set Y, where X and Y are finite subsets of $\mathbb{N}$.*

This set of mappings will be useful to reindex the vertex of polygonal curves.

Definition 1 *The discrete Fréchet distance between two polygonal curves $\mathcal{P}$ and $\mathcal{Q}$ is:*

$$d_F(\mathcal{P},\mathcal{Q}) = \min_{(\kappa,\lambda)} \parallel \mathcal{P}\circ\kappa - \mathcal{Q}\circ\lambda \parallel_\infty$$

where the pairs (κ,λ) range over

$$Mon_{m,n} = Mon([1:m+n],[0:m]) \times Mon([1:m+n],[0:n])$$

In our case, $\mathcal{P}$ and $\mathcal{Q}$ are polygonal curves in $\mathbb{R}^3$ represented as the list of their vertex, the distance under consideration is the discrete Fréchet distance and $G = SO(3,\mathbb{R})$ is the group of rotations in $\mathbb{R}^3$.

Our problem is to decide whether $G(\mathcal{P},\mathcal{Q},\epsilon,d_F)$, the set of all g in G such that $d_F(\mathcal{P},g\mathcal{Q}) \leq \epsilon$, is empty or not.

Since it is easier to work on points than to work with curves we introduce (G,ϵ)-transporter set for points p and q in $\mathbb{R}^3$:

$$\tau_{p,q}^{G,\epsilon} = \{g \in G \mid \parallel p - gq \parallel \leq \epsilon\}$$

In [23, 22] the following straightforward relation between $G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F)$ and transporter sets is given:

$$G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F) = \bigcup_{(\kappa,\lambda)\in Mon_{m,n}} \bigcap_{s\in[1:m+n]} \tau^{G,\epsilon}_{p_{\kappa(s)},q_{\lambda(s)}}$$

Deciding the emptiness of $G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F)$ is equivalent to deciding, for each κ, λ in $Mon_{m,n}$, the emptiness of $\bigcap_{s\in[1:m+n]} \tau^{G,\epsilon}_{p_{\kappa(s)},q_{\lambda(s)}}$.

Transporter polynomials To describe $\tau^{G,\epsilon}_{p_{\kappa(s)},q_{\lambda(s)}}$ with polynomials, the group $SO(3,\mathbb{R})$ is parametrized by unit quaternions. We will also use the following mapping:

$$\begin{array}{ccc} \mathbb{R}^3 & \rightarrow & \mathbb{H} \\ (x,y,z) & \mapsto & (1,x,y,z) \end{array}$$

The matrix of rotation $g_{(w,x,y,z)}$ is:

$$\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & w^2+x^2-y^2-z^2 & 2xy-2wz & 2xz+2wy \\ 0 & 2xy+2wz & w^2-x^2+y^2-z^2 & 2yz-2wx \\ 0 & 2xz-2wy & 2yz+2wx & w^2-x^2-y^2+z^2 \end{array}\right]$$

A $(SO(3,\mathbb{R}),\epsilon)$ transporter polynomial for p and q is calculated as follows:

$$g^{\epsilon}_{p,q} = \epsilon^2 - \| \begin{pmatrix} 1 \\ p_x \\ p_y \\ p_z \end{pmatrix} - g_{(w,x,y,z)} \begin{pmatrix} 1 \\ q_x \\ q_y \\ q_z \end{pmatrix} \|^2$$

where ϵ, (p_x, p_y, p_z), and (q_x, q_y, q_z) are rationals.

This leads to the following polynomial system in four unknowns

$$\left\{\begin{array}{rcl} w^2+x^2+y^2+z^2 & = & 1 \\ g^{\epsilon}_{p_{\kappa(1)},q_{\lambda(1)}} & \geq & 0 \\ & \vdots & \\ g^{\epsilon}_{p_{\kappa(m+n)},q_{\lambda(m+n)}} & \geq & 0 \end{array}\right.$$

for each κ, λ in $Mon_{m,n}$.

Other groups of transformation We can do the same with the group of translations as the group of acceptable transformations by using the following matrix:

$$\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{array}\right]$$

Applying this matrix to $(1,x,y,z)$ we get $(1, x+a, y+b, z+c)$ and back in $\mathbb{R}^3$ we get $(x+a, y+b, z+c)$ which is $(x,y,z)+(a,b,c)$.

We can also use non-uniform scalings (or uniform scalings if $\lambda_x = \lambda_y = \lambda_z = \lambda$):

$$\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & \lambda_x & 0 & 0 \\ 0 & 0 & \lambda_y & 0 \\ 0 & 0 & 0 & \lambda_z \end{array}\right]$$

To guarantee that we work on the group of scalings we must add the following constraint which prevents any λ from vanishing:

$$\lambda_x \lambda_y \lambda_z \Lambda = 1$$

where Λ is a new variable.

These transformations can be combined and several polynomial systems of equations and non-strict inequalities can be generated. Some restrictions can be imposed:

- one can choose to consider translations following a fixed direction; this is equivalent to fix 2 variables among a, b and c and lead to consider polynomial systems with 5 variables.
- one can choose between uniform or non-uniform scalings: this leads to polynomial systems in 11 or 9 variables.
- mixing the above choices is also possible: we get polynomial systems in 7 variables obtained by considering translations with respect to a fixed direction and uniform scalings.

The polynomial systems we studied and a Maple code generating them can be downloaded at the URL:

`http://www-calfor.lip6.fr/~safey/Applications/`

The implementation To solve this problem the algorithm **Algorithm** 2 has been implemented in the RAG'Lib Maple Library [30]. Each part of the algorithm works as a black box.

We begin our walk through subsets of $\{1, \ldots, s\}$ by subsets of size one, and if a subset I gives no solution we do not test any subset containing I. The routine used to find at least one point in each connected component of an algebraic variety is an experimental version of RAG'Lib's function called `a_component` which mixes the algorithms provided in [32] and [31]. It uses the softwares `Gb` implemented by J.-C. Faugère for Gröbner bases computations and `RS` implemented by F. Rouillier for computing rational parametrizations of zero-dimensional algebraic sets (see [13]). To evaluate the sign of multivariate polynomials at real algebraic points given by a rational parametrization, we substitute classically the parametrization to the variables in the polynomials so that the problem is reduced to evaluate the sign of univariate polynomials at real roots of an other univariate polynomial. This is actually the blocking part of our algorithm on this problem.

Experimental protocol We used our algorithm to solve such problems in four (in the case of rotations) seven (in the case of rotations and translations) and eleven (in the case of rotations, translations and scalings) unknowns and s constraints.

The examples were generated with the following protocol. We first decide the number of constraints s and the precision of the matching ϵ. Then if we want our system to have a solution:

- a first polygonal curve $\mathcal{P}$ is generated in the cube $[-1, 1]^3$
- we decide a perturbation $\delta < \epsilon$
- a second polygonal curve $\mathcal{Q}_0$ is generated from $\mathcal{P}$ by adding an arbitrary vector of size δ to each point of $\mathcal{P}$

- we choose a transformation and we apply it to $\mathcal{Q}_0$ to get $\mathcal{Q}$

If we do not want our system to have a solution, $\mathcal{P}$ and $\mathcal{Q}$ are both randomly generated. Once we have $\mathcal{P}$ and $\mathcal{Q}$ we only study the system:

$$\left\{\begin{array}{rcl} w^2+x^2+y^2+z^2 & = & 1 \\ \lambda_x\lambda_y\lambda_z\Lambda & = & 1 \\ g^{\epsilon}_{p_1,q_1} & \geq & 0 \\ & \vdots & \\ g^{\epsilon}_{p_s,q_s} & \geq & 0 \end{array}\right.$$

The first two constraints depend on the acceptable transformation and appear only if necessary.

Our tests have been done with $s = 9$ on systems with 4, 7 and 11 variables.

Experimental results The computations have been performed on PC Pentium III 1 GHz with 512 Mbytes of RAM. The evaluation of the sign of the constraints by the method we describe above is a blocking stage. A more efficient one is provided in [26] where the constraints modulo the studied zero-dimensional system are represented by a rational function instead of a polynomial. We did not filter the output, and the execution time we give below is the time needed to calculate the zero-dimensional systems encoding at least one point in each connected component of the real algebraic sets studied during the walk of **Algorithm** 2.

The software `QEPCAD` (see [11]) can not solve the polynomial systems we studied after two weeks of computations on the same machine.

Systems with 4 variables and 9 constraints corresponding to the group of translations are solved approximately in 5 hours and 45 minutes. Each algebraic system studied during the walk of **Algorithm** 2 is solved in at most 2 minutes and a half. The largest degree of the returned zero-dimensional sets is 196. Thus, the case where the group of transformations is the the group of rotations seems to be reachable by algebraic techniques.

Considering the group of rotations and translations with respect to a fixed direction generates polynomial systems with 5 variables and 9 constraints which are solved by our implementation in 1 hour. Each algebraic system studied during the walk of **Algorithm** 2 is solved in at most 40 seconds. The largest degree of the returned zero-dimensional sets is 140. Thus, this case also is reachable by algebraic techniques.

The same conclusion occurs when considering the group of rotations and uniform scalings. The generated polynomial systems contain 6 variables and are solved in 20 minutes. Each algebraic systems studied during the walk of **Algorithm** 2 is solved in at most 10 seconds. The largest degree of the returned zero-dimensional sets is 80. Thus, the case where the group of transformations is the the group of rotations seems to be reachable by algebraic techniques.

Considering the group of translations (without restrictions) or the group of scalings lead to polynomial systems which can not be solved by our techniques.

References

[1] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Proceedings MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.

[2] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[3] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[4] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[5] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties: geometry and algorithms. Technical report, Humboldt Universität, 2003.

[6] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. The light is polar. *Unpublished manuscript*, 2003.

[7] S. Basu. *Algorithms in semi-algebraic geometry.* PhD thesis, New-York University, 1996.

[8] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6):1002–1045, 1996.

[9] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition.* Springer-Verlag, 1998.

[10] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry.* Springer-Verlag, 2003.

[11] C. Brown. Qepcad, quantifier elimination by partial cylindrical algebraic decomposition. http://www.cs.usna.edu/ qepcad/B/QEPCAD.html, 2002.

[12] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Lecture notes in computer science*, 33:515–532, 1975.

[13] J.-C. Faugère and F. Rouillier. FGb/RS package. http://fgbrs.lip6.fr, 2003.

[14] M. Giusti, K. Hägele, J. Heintz, J.-E Morais, J.-L. Montaña, and L.-M. Pardo. Lower bounds for Diophantine approximation. In *Proceedings of MEGA'96*, number 117, 118 in Journal of Pure and Applied Algebra, pages 277–317, 1997.

[15] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.

[16] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *Proceedings of AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[17] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[18] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[19] J. Heintz, M.-F. Roy, and P. Solernò. On the complexity of semi-algebraic sets. In *Proceedings IFIP'89 San Francisco, North-Holland*, 1989.

[20] J. Heintz, M.-F. Roy, and P. Solernò. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.

[21] G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques*. PhD thesis, École polytechnique, 2001.

[22] A. Mosig. *Efficient algorithms for shape and pattern matching*. PhD thesis, Bonn University, to appear, 2004.

[23] A. Mosig and M. Clausen. Approximately matching polygonal curves with respect to the fréchet distance. *submitted to Computational Geometry – Theory and Applications*, 2004.

[24] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. *Journal of symbolic computation*, 13, 1992.

[25] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *AAECC Journal*, 9(5):433–461, 1999.

[26] F. Rouillier. On computing and using the rational univariate representation for solving zero-dimensional semi-algebraic systems. Technical report, INRIA, 2004.

[27] F. Rouillier and P. Zimmermann. Efficient Isolation of a Polynomial Real Roots. Rapport de recherche, INRIA, February 2001.

[28] M.-F. Roy. Basic algorithms in real algebraic geometry : from sturm's theorem to the existential theory of reals. In *Lectures on real geometry in memoriam of Mario Raimondo*, volume 23 of *Expositions in mathematics*, pages 1–67. New-York, de Gruyter, 1996.

[29] M. Safey El Din. *Résolution réelle des systèmes polynomiaux de dimension positive*. PhD thesis, Université Paris 6, January 2001.

[30] M. Safey El Din. RAGLib. http://www-calfor.lip6.fr/∼safey/RAGLib, 2003.

[31] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. ISSAC'03 Proceedings, 2003.

[32] M. Safey El Din and É. Schost. Properness defects of projections and computation of one point in each connected component of a real algebraic set. *to appear in Journal of Discrete and Computational Geometry*, 2004.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399